

System Security Administration Manual

Enterprise Income Verification
System

U.S. Department of Housing and
Urban Development

Version 4.0 September 2005

Revision History

Note: This is an extract from the EIV Operations Manual, portions of which are restricted.

Version	Date	Comments required	Approvals required
Version 1.0	01/30/03	Initial Draft	
Version 1.1	03/24/03	Build 2 Updates incorporated	
Version 2.0	03/31/03	Build 2 Release	
Version 2.1	05/14/03	Build 2.1 Updates incorporated	
Version 3.0	08/01/03	Build 3 Release	
Version 3.0.1	11/07/03	Build 3 Patch Release	
Version 3.0.3	02/24/04	Build 3.0.3 Patch Release	
Version 3.1	05/18/04	Build 3.1 Release	
Version 3.1	08/06/04	Build 3.1 Release Updates	
Version 3.2	02/03/05	Build 3.2 Release	
Version 4.0	09/16/05	Build 4.0 Release	

Table of Contents

Preface	4
Document Overview	4
How This Manual is Organized	4
Who Should Use This Manual?	4
Related Documentation	5
Acronyms and Abbreviations	5
 Chapter 1, Introduction	 6
System Overview	6
Contingencies and Alternate Modes of Operation	8
Security	8
User Accounts	8
Security Awareness	9
Security Procedures	9
Audits and User Activity Logging	10
 Chapter 2, Audit Reports	 11
Viewing the User Session and Activity Audit Report	12
Viewing the User Activity Log Audit Report	14
Viewing the Tenant Data Access Audit Report	16
Viewing the Failed Login Audit Report	19
Viewing the Denied User Access Audit Report	20
 Chapter 3, User Role History Report	 22
 Appendix A – Abbreviations and Acronyms	 25

List of Tables and Figures

Figure 1 – EIV System Interactions	7
Table 2 – User Session and User Activity Report Definitions	13
Table 3 – User Activity Log Report Definitions	15
Table 4 – Tenant Data Access Report Field Definitions	18
Table 5 – Failed Login Report Definitions	20
Table 6 – Denied User Access Report Field Definitions	21

Preface

Document Overview

Welcome to the EIV Operations Manual. The purpose of this manual is to provide instructions for HUD personnel responsible for system, security, and user administration of the Enterprise Income Verification (EIV). It details business operational procedures for successfully performing administration tasks through EIV user interface.

How This Manual is Organized

Listed below are each of the chapters contained in this manual, along with a brief description of its content:

- **Chapter 1, Introduction** – An overview of EIV, including the hardware, software, and system architecture.
- **Chapter 2, Audit Reports** – Provides instruction on using the audit reporting functionality for security administration.
- **Chapter 3, User Role History Report** – Provides the history of the roles assigned to a user
- **Appendix A, Abbreviations and Acronyms** – Provides a list of commonly used abbreviations and acronyms.

Who Should Use This Manual?

This manual is intended for users with the EIV system Security Administration role.

If you have other roles, you may need to access other documents in EIV library to learn more about them. For more information about the content of the EIV library, refer below to the [Related Documentation](#) section of this document.

This manual assumes the resources assigned to these roles have the following knowledge or expertise:

- Working knowledge of Microsoft Windows.
- Operational understanding of PCs.
- Operational understanding of Internet browsers.
- Understanding of basic network concepts.

- Understanding of HUD program terminology, policies, and procedures.

Related Documentation

This section provides a list of related documentation. The EIV library includes the following document:

- ***EIV User Manual*** – For users of the EIV wage and income functionality, this manual provides step-by-step instructions. Users should be familiar with PCs, Microsoft Windows, and their browser software.

Acronyms and Abbreviations

A glossary of acronyms and abbreviations is included as **Appendix A** of this document.

Chapter 1, Introduction

This chapter provides an overview of EIV. Topics discussed include:

- System Overview,
- Contingencies and Alternate Modes of Operation,
- EIV operates 24 hours a day, 7 days per week (except first weekend of each month due to PIC dependency). However, best conditions for use are during weekdays because batch processing will be run **over night and during weekends, which may impact system responsiveness. Notices of planned outages for system maintenance (as well as other guidance) will be posted on the EIV Information web site.**

<http://www.hud.gov/offices/pih/programs/ph/rhiip/uiv.cfm>

- Security

System Overview

EIV provides a portal to tenant income information in the form of household income data, as well as several income-based reports. EIV is a Web-based system, allowing access to information across secure Internet connections to the HUD application server using Microsoft Internet Explorer Version 6.0 and higher.

Tenant income data in the EIV system comes from a variety of sources including the following:

- **Form HUD-50058 Database** – provides tenant-reported household information (name, SSN, program type, address, projected income, etc.).
- **NDNH** – US Department of Health and Human Services, National Directories of New Hires (NDNH) provides information concerning employment information (W4), wages, unemployment benefits, for participating PIH Public Housing and voucher programs.

- **Social Security Administration** – provides information concerning Social Security and supplemental security income payments for tenants who participate in PIH Public Housing and voucher programs. In addition, SSA provides feedback to EIV concerning problems with tenant ID information.

The EIV system is related to the PIC system, particularly the 50058 module. To simplify security administration, only users who have rights to access PIC may access EIV. However, the EIV security module controls the extent of rights within EIV. Figure 1 illustrates these primary system interactions.

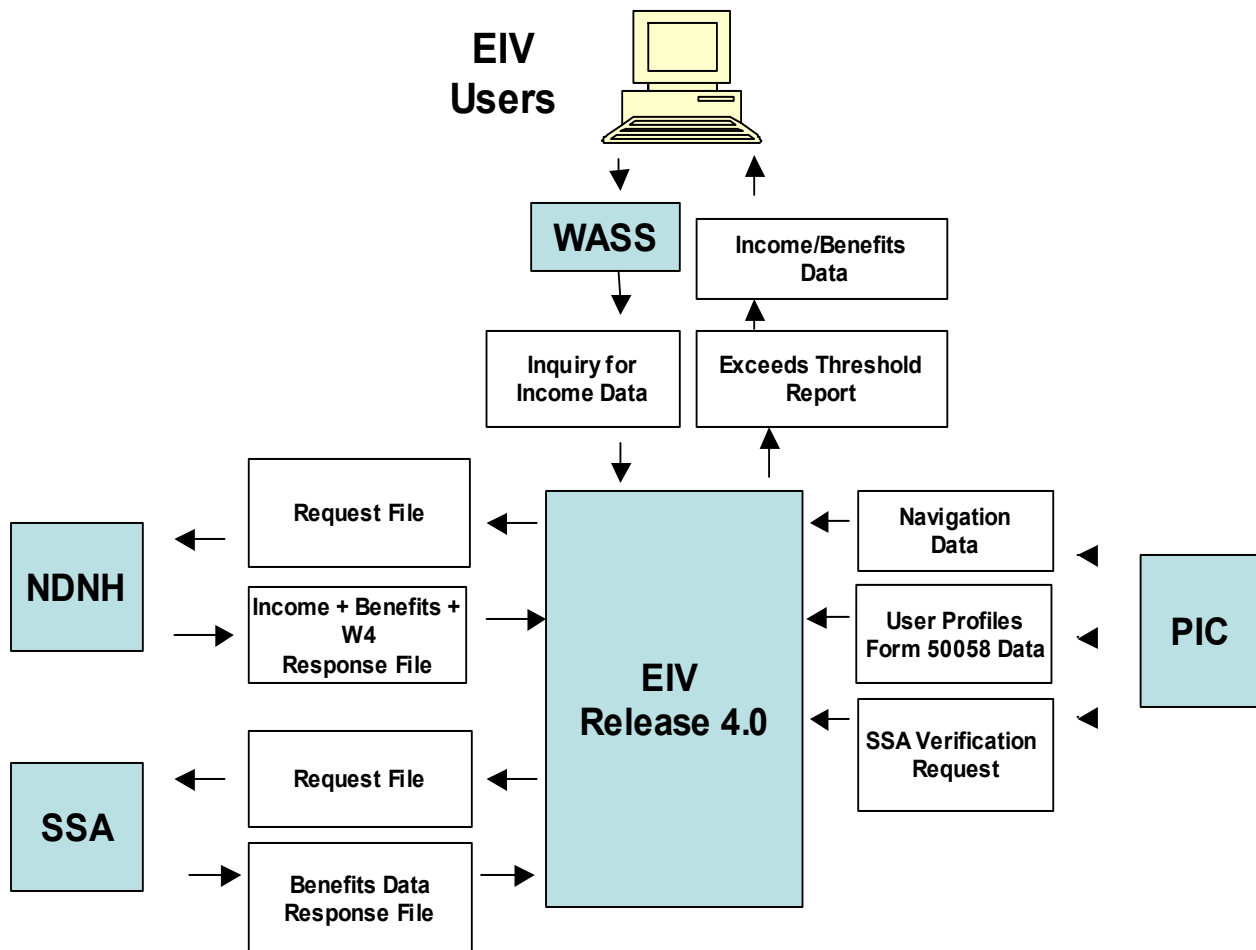


Figure 1 – EIV System Interactions

Contingencies and Alternate Modes of Operation

EIV operates 24 hours a day, 7 days per week (except first weekend of each month due to PIC dependency). However, best conditions for use are during weekdays because batch processing will be run over night and during weekends, which may impact system responsiveness. **Notices of planned outages for system maintenance (as well as other guidance) will be posted on the EIV Information web site.**

<http://www.hud.gov/offices/pih/programs/ph/rhiip/uiv.cfm>

Security

EIV contains personal information concerning tenants that is covered by the Privacy Act such as wage and income data about private individuals, as well as identifying information such as Social Security Number, address, and employment information. This information may only be used for limited official purposes, which are tenant recertification and oversight of the tenant recertification process (which includes use by OIG and GAO). It does not include sharing with governmental entities not involved in the recertification process. Users are encouraged to refer any non-standard requests for access to HUD management and to report any unauthorized disclosure of EIV data to the manager of the HUD Privacy Act Officer or to the Office of Inspector General. If it appears that the system has been “hacked”, that should be reported to the HUD Help Desk (1-888-297-8689).

All EIV users must adhere to the Rules of Behavior which is to be found as part of the User Agreement that is being implemented with EIV 4.0. A copy of the User Agreement is posted on the EIV Information web site. The rules clearly delineate responsibilities of, and expectations for, all individuals with access to the EIV system. Non-compliance with these rules will be disciplined through sanctions commensurate with the level of infraction. Sanctions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination depending on the severity of the violation.

Access to tenant data is logged as part of the effort to protect the data and provide traceability should a questionable event occurs.

User Accounts

User accounts for EIV should be provided on a need-to-know basis, with appropriate approval and authorization. All EIV User Administrators are to maintain a file for each user, the access authorizations signed by the responsible manager, the EIV User Agreement signed by the user and a user-signed copy of the EIV Rules of Behavior (which is part of the revised EIV User Agreement being distributed with the implementation of EIV 4.0). Effective after the first full quarter of EIV operations (January 1, 2006), User Administrators will be required to certify each

Introduction

quarter that users have appropriate rights in EIV. They will be unable to make that certification if the documentation is not in the file. User accounts that have not been certified within 30 days thereafter will lose their EIV roles and will not be able to access EIV.

EIV uses a role-based authorization scheme to grant users access to the EIV content. An EIV user belongs to a security level based on their organization (Headquarters, Hub, TARC, Field Office, or PHA), and a role, based on their job responsibilities and functional needs.

- **Security level** – A user's access to data is limited to their organization level (Headquarters, Hub, TARC, Field Office, or PHA), and their specific organization.
 1. Headquarters user can see nationwide data.
 2. Hubs, TARCs, and Field Offices are still restricted to their respective areas.
 3. The EIV system will support the assignment of access to multiple PHAs under one WASS ID. Such an assignment will only be made to those PHA employees or contractors who access EIV must have that need documented in the User Administration file signed by the head of the additional PHA.
- **Role** – A role is an assigned right to use a distinct part of a system's functionality. In EIV, roles include Occupation Specialist, User Administrator, Systems Administrator and Security Administrator. A user's access to functionality is determined by the role or roles to which they are assigned. Each role provides access to a set of functions appropriate to that user type. For example, a PHA Occupancy Specialist can access income data features, but does not have access to user administration, security administration, or system administration features. A user can be assigned one or more roles; the functionality the user can access is a cumulative set of all features given to all roles to which the user is assigned. Users are assigned roles that are limited in scope to their organizational level. (PHA, Field Office, TARC, HUB, and Headquarters) and those below it.

Security Awareness

New EIV users are to receive as part of their training EIV users are to receive a familiarization with the requirements of the Privacy Act. Users are required to have annual security awareness training to refresh and update that initial training. Potential EIV users must sign the EIV Access Request to signify that they understand and accept the EIV Rules of Behavior. Guidance concerning security has been posted on the EIV web page.

<http://www.hud.gov/offices/pih/programs/ph/rhiip/uivsystem.cfm>

The complete text of the Privacy Act is available at:

<http://www.usdoj.gov/foia/privstat.htm>

Security Procedures

The WASS system, through which all users will access EIV, provides a timeout that disables access to the system after a 30-minute pause in use. That, in and of itself is not enough protection. Users should not leave their PCs unattended when access to WASS or any system accessible through WASS is possible. Users should be aware that logging out from EIV to WASS is not sufficient in that clicking on the WASS link to EIV will allow reentry to the EIV system. The

activation of a screen saver is one way to protect access through an untended PC. Another is to close the browser window. It is possible to do so by going through the WASS closing routine which includes saying Yes to the question of whether to close the window. It is easier and quicker to close the browser window by clicking the X in the upper-right-hand corner of the screen.

Other security considerations relate to the physical security of the area where the EIV system is used, and policies and procedures that are enforced by management.

Guidance concerning security practices, governing the work area and storage of paper records containing personal information and their destruction when they no longer are needed, may be found at the EIV Information Web site.

Audits and User Activity Logging

Users of EIV should be aware that successful login/logoff, login failure and tenant data access activities within the system are logged for security audit and reporting purposes. These audits may include records of attempts to access data to which the user is not authorized, as well as successful access of sensitive data to which the user is authorized.

Changes to the user roles and user certification transactions are also logged.

Chapter 2, Audit Reports

This chapter discusses the audit reporting functions in EIV. Audit reports allow the Security Administrator to generate and review reports summarizing system and data use. The following reports are discussed in this chapter:

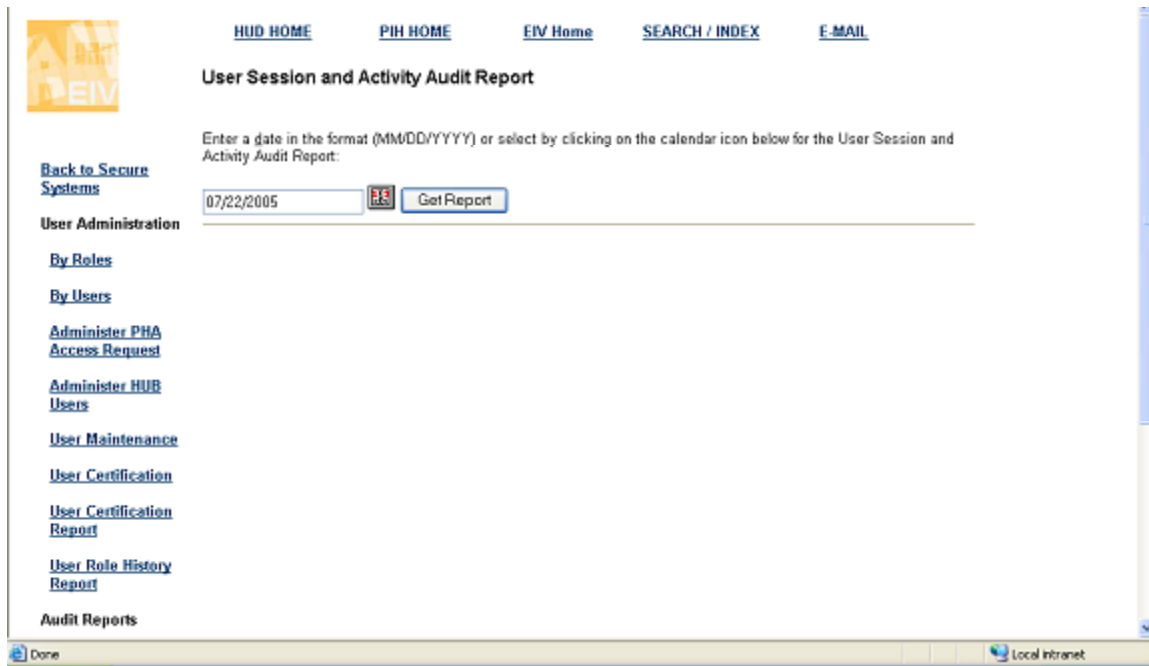
- *Viewing the User Session and Activity Audit Report*
- *Viewing the User Activity Log Audit Report*
- *Viewing the Tenant Data Access Audit Report*
- *Viewing the Failed Login Audit Report*
- *Viewing the Denied User Access Audit Report*

Viewing the User Session and Activity Audit Report


This report details each user session and the pages accessed during the session. To view the User Session and Activity audit report, complete the following steps:

- Click the [User Session and Activity](#) link.

The system displays the **User Session and Activity Audit Report** page. This page looks like this:



The screenshot shows the 'User Session and Activity Audit Report' page. At the top, there are navigation links: HUD HOME, PIH HOME, EIV Home, SEARCH / INDEX, and E-MAIL. Below these is the title 'User Session and Activity Audit Report'. A text box prompts the user to 'Enter a date in the format (MM/DD/YYYY) or select by clicking on the calendar icon below for the User Session and Activity Audit Report:'. A date field contains '07/22/2005' and a calendar icon is visible. A 'Get Report' button is next to the date field. On the left side, there is a sidebar with links: 'Back to Secure Systems', 'User Administration' (with sub-links 'By Roles', 'By Users', 'Administer PHA Access Request', 'Administer HUB Users', 'User Maintenance', 'User Certification', 'User Certification Report', and 'User Role History Report'), and 'Audit Reports'. The bottom of the page shows a Windows taskbar with 'Done' and 'Local intranet' icons.

- Enter a date in the format (MM/DD/YYYY), or select a date by clicking on the calendar () tool.
- Click **Get Report**.

Audit Reports

The system displays the **User Session and Activity Audit Report** results page. This page looks like this:

HUD HOME PIH HOME EIV Home SEARCH / INDEX E-MAIL

User Session and Activity Audit Report

Enter a date in the format (MM/DD/YYYY) or select by clicking on the calendar icon below for the User Session and Activity Audit Report:

07/25/2005 Get Report

User Administration

[Back to Secure Systems](#)

[By Roles](#)

[By Users](#)

[Administer PHA Access Request](#)

[Administer HUB Users](#)

[User Maintenance](#)

[User Certification](#)

[User Certification Report](#)

[User Role History Report](#)

Audit Reports

User ID	First Name	Last Name	Logon Timestamp	Logoff Timestamp	IP Address	Details
HEMD1	SSCHD1	EV	Jul 25 2005 7:55AM		10.210.44.98	

- To view details for a particular use/r session, click the **View Detail** tool ().

Definitions for each field in this report are provided in the following table:

Report Heading	Definition
User ID	The assigned access ID for a user.
First Name	First name of a user.
Last Name	Last name of a user.
Logon Timestamp	The date and time the user logged on.
Logoff Timestamp	The date and time the user logged off.
IP Address	The address of the accessing computer.
Details	Details all activity for the user.

Table 2 – User Session and User Activity Report Definitions

Viewing the User Activity Log Audit Report

This report is a superset of the User Session and Activity Audit report, and details all user actions. To view the User Activity Log audit report, complete the following steps:

- Click the [User Activity Log](#) link. The system displays the **User Activity Log Audit Report** page.

This page looks like this:

HUD HOME PIH HOME EIV Home SEARCH / INDEX E-MAIL

User Activity Log Audit Report

Enter a date in the format (MM/DD/YYYY) or select by clicking on the calendar icon below for the User Activity Log Audit Report:

07/22/2005 


[Back to Secure Systems](#)

User Administration

- [By Roles](#)
- [By Users](#)
- [Administer PHA Access Request](#)
- [Administer HUB Users](#)
- [User Maintenance](#)
- [User Certification](#)
- [User Certification Report](#)
- [User Role History Report](#)

Audit Reports

Done Local intranet

- Enter a date in the format (MM/DD/YYYY), or select one by clicking the calendar () tool.
- Click **Get Report**.

The system displays the **User Activity Log Audit Report** page:

Definitions for each field in this report are provided in the following table:

Report Field Heading	Definition
User ID	The assigned access ID for a user.
Name	The user's first and last name.
Access Timestamp	The date and time access was attempted.
IP Address	The address of the accessing computer.
Request URL	The command link the user accessed.
Request Method	What the user did (e.g., get data, post data).

Table 3 – User Activity Log Report Definitions



Viewing the Tenant Data Access Audit Report

This report provides a list of all EIV system users who have access tenant wage and income data within a specified period of time. To view the Tenant Access audit report, complete the following steps:

- Click the [Tenant Data Access](#) link.

The system displays the **Tenant Data Access Audit Report** page. This page looks like this:

Control the content of the report using the following criteria:

- **Start Date – (Required)** defines the beginning date for the reporting period. The Start Date value cannot be greater than the End Date value. Enter a date in the format (MM/DD/YYYY), or select one by clicking on the calendar () tool.
- **End Date – (Required)** defines the ending date for the reporting period. The End Date value must be greater than the Start Date value. Enter a date in the format (MM/DD/YYYY), or select one by clicking on the calendar () tool.
- **Tenant SSN – (Optional)** designates the social security number of the tenant you want included in the report content. Use this criterion when you want to limit report content to a specific social security number.
- **Tenant Last Name – (Optional)** designates the last name of the tenant you want included in the report's content. Use this criterion when you want to limit report content to a specific tenant's name.

Audit Reports

- Enter the report filter criteria and click **Get Report**.

The system displays the **Tenant Data Access Audit Report** page.

Tenant Data Access Audit Report

Specify the inclusive start and end dates for the time period. You can also enter either Last Name or SSN of a tenant. Specify dates in the format select by clicking on the calendar tool.

* Start Date: 07/07/2005
* End Date: 07/08/2005
Tenant SSN:
Tenant Last Name:
* Select a Participant Code: FL001 Jacksonville Get Report

Printer-friendly Version

User ID	User Name	Activity	Date	Duration (min:ss)	Tenant Name	SSN	PHA	Program
M00333	SS0333 EVTest	PHA	07/08/2005 11:49:15	20:00	JOHN DOE	266-26-1903	FL001	P
jndoe	Marg Smith	HQ	07/08/2005 11:48:26	20:00	JOHN DOE	591-29-8229	FL001	VO
M00335	SS0335 EVTest	PHA	07/08/2005 10:34:40	20:00	TEST NAME	XXX-XX-XXXX	FL001	P
M00335	SS0335 EVTest	PHA	07/08/2005 10:34:12	20:00	HARRY H CRAIG	XXX-XX-XXXX	FL001	P
M00335	SS0335 EVTest	PHA	07/08/2005 10:34:06	20:00	LAKE ROBERT	XXX-XX-XXXX	FL001	P
sxmakine	Makineni Smitha	HQ	07/08/2005 10:33:33	20:00	SMITH Y JAMES	XXX-XX-XXXX	FL001	VO

Definitions for each field in this report are provided in the following table:

Report Field Heading	Definition
User ID	The assigned access ID for a user.
User Name	The user's first and last name.
Activity	The identity of the PHA at which the activity took place.
Date	The date and time the access was attempted.
Duration (Min:Sec)	The amount of time spent viewing the page. The amount of time is expressed as a minutes and seconds value. The elapsed time counter begins when the Household Income Details page is launched and stops when the user accesses another page. In the event that another page is not accessed, the system assigns a default elapsed time value of twenty (20) minutes.
Tenant Name	The tenant's name.
SSN	The tenant's social security number.
PHA	The identity of the PHA responsible for the administration of the tenant's records.
Program Type	The type of housing project in which the tenant is participating, as applicable.
Project	The type of project in which the tenant is living, as applicable.

Table 4 – Tenant Data Access Report Field Definitions

Complete the following actions to access the Printable View:

To generate a printer-friendly version of the report,

- Click the [Printer-friendly version](#) button.

The system generates a printer-friendly version of the report and displays it in a separate Browser window.

- Click the Browser's print icon to produce a paper version of the report. When you have finished printing the report, close the browser window.


Viewing the Failed Login Audit Report

This report tracks logon attempts where a user has attempted log on entering an incorrect ID or password. To view the Failed Login audit report, complete the following steps:

- Click the [Failed Login](#) link.

The system displays the **Failed Login Audit Report** page. This page looks like this:

The screenshot shows the 'Failed Login Audit Report' page. At the top, there are navigation links: HUD HOME, PIH HOME, EIV Home, SEARCH / INDEX, and E-MAIL. Below these is the EIV logo. The main heading is 'Failed Login Audit Report'. A text prompt says: 'Enter a date in the format (MM/DD/YYYY) or select by clicking on the calendar icon below for the Failed Login Audit Report:'. Below this is a text input field containing '07/25/2005', a calendar icon, and a 'Get Report' button. On the left side, there is a sidebar with links: 'Back to Secure Systems', 'User Administration' (with sub-links: 'By Roles', 'By Users', 'Administer PHA Access Request', 'Administer HUB Users', 'User Maintenance', 'User Certification', 'User Certification Report', 'User Role History Report'), and 'Audit Reports'. The bottom status bar shows 'Done' and 'Local intranet'.

- Enter a date in the format (MM/DD/YYYY), or select one by clicking on the calendar  tool.
- Click **Get Report**.

The system displays the **Failed Login Audit Report** page. This page looks like this:

This screenshot shows the same 'Failed Login Audit Report' page, but with the results table displayed. The date in the input field is '07/20/2005'. The table is titled 'Failed Login Audit Report for 07/20/2005' and has five columns: User ID, First Name, Last Name, Logon Timestamp, and IP Address. The table contains two rows of data for the user 'exuser10'.

User ID	First Name	Last Name	Logon Timestamp	IP Address
exuser10			Jul 20 2005 10:48AM	10.210.44.98
exuser10			Jul 20 2005 10:49AM	10.210.44.98

Audit Reports

Definitions for each field in this report are provided in the table below:

Report Field Heading	Definition
User ID	The assigned access ID for a user.
First Name	The user's first name.
Last Name	The user's last name.
Logon Timestamp	The date and time the log on was attempted and failed.
IP Address	The address of the accessing computer.

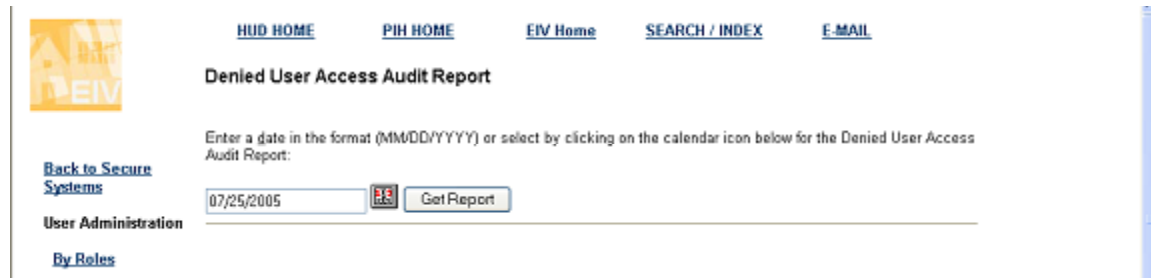
Table 5 – Failed Login Report Definitions


Viewing the Denied User Access Audit Report

This report tracks access attempts to tenant income records that are not in the PHA (e.g., an income verification specialist enters a social security number for a tenant record that is not part of the PHA). To view the Denied User Access audit report, complete the following steps:


- Click the [Denied User Access](#) link.

The system displays the **Denied User Access Audit Report** page. This page looks like this:



- Enter a date in the format (MM/DD/YYYY), or select one by clicking on the calendar  tool.
- Click **Get Report**.

The system displays the **Denied User Access Report** page. This page looks like this:




[HUD HOME](#) [PIH HOME](#) [Q & A](#) [SEARCH / INDEX](#) [E-MAIL](#)

Denied User Access Audit Report

Enter a date in the format (MM/DD/YYYY) or select by clicking on the calendar icon below for the Denied User Access Audit Report:

[Log Off](#)

Search Income Records



[By Head of Household Information](#)
[By Reexamination Month](#)

Denied User Access Audit Report for 02/24/2005				
User ID	Name	Access Timestamp	IP Address	Resource
mxbyrd	myra byrd	Feb 24 2005 7:17PM	170.97.67.76	/uiv/tenantsearch
vxgarza	Viola Garza	Feb 24 2005 7:17PM	170.97.67.76	/uiv/tenantsearch
rxcrow	Robert E Crow	Feb 24 2005 6:59PM	170.97.167.46	/uiv/tenantsearch
axhaghesh	Ali Haghshenas	Feb 24 2005 6:58PM	170.97.167.46	/uiv/tenantsearch

Definitions for each field in this report are provided in the table below:

Report Field Heading	Definition
User ID	The assigned access ID for a user.
Name	The user's first and last name.
Access Timestamp	The date and time the access was attempted.
IP Address	The address of the accessing computer.
Attempted Function	Identifies what function was being accessed.

Table 6 – Denied User Access Report Field Definitions

Chapter 3, User Role History Report

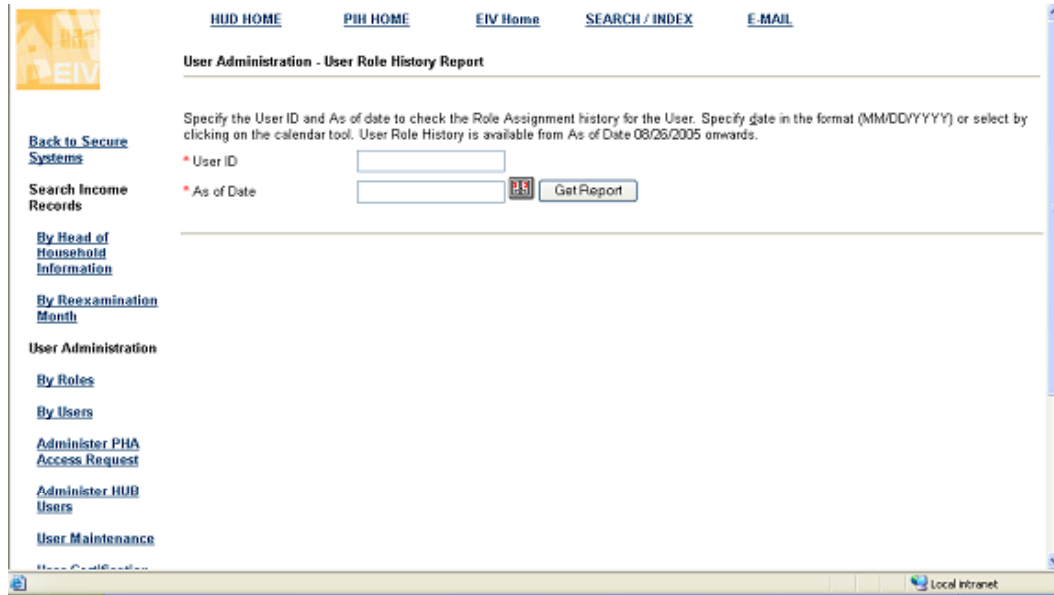
User Administrators can view the **Role Assignment history** for any User using the [User Role History Report](#) feature

To generate the [User Role History Report](#), follow these steps:

- Click the [User Role History Report](#) link in the left-hand navigation panel.

The system displays the **User Administration - User Role History Report** page, which looks like this:

- Put in the **User ID**. Type in a date or click the **Calendar link** () and select a date in the **As of Date** textbox. Click the **Get Report** button




HUD HOME **PIH HOME** **EIV Home** **SEARCH / INDEX** **E-MAIL**

User Administration - User Role History Report

Specify the User ID and As of date to check the Role Assignment history for the User. Specify date in the format (MM/DD/YYYY) or select by clicking on the calendar tool. User Role History is available from As of Date 08/26/2005 onwards.

* User ID

* As of Date 

[Back to Secure Systems](#)

Search Income Records

[By Head of Household Information](#)

[By Reexamination Month](#)

User Administration

[By Roles](#)

[By Users](#)

[Administer PHA Access Request](#)

[Administer HUD Users](#)

[User Maintenance](#)

Local Intranet

Audit Reports

The system displays the **User Administration - User Role History Report** page with the selected Users' Role History as of the specified date. The following fields are displayed on the report:

- Role
- Action
- Participant Code
- Updated by User
- Update Date

HUD HOME **PIH HOME** **EIV Home** **SEARCH / INDEX** **E-MAIL**

User Administration - User Role History Report

Specify the User ID and As of date to check the Role Assignment history for the User. Specify date in the format (MM/DD/YYYY) or select by clicking on the calendar tool. User Role History is available from As of Date 08/26/2005 onwards.

* User ID:

* As of Date:

User ID: heav01 **User Name:** EIVTest SSOH01

Role	Action	Participant Code	Updated By User	Update Date
HQ Occupancy	Approved	NA	HEIV08 EIVTest SSOH08	2005-07-18 15:08:19.847
HQ User Admin	Approved	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:50.88
HQ System Admin	Revoked	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:50.847
HQ Security Admin	Revoked	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:50.83
HQ Senior Mgt	Revoked	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:50.817
HQ OIG	Revoked	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:50.8
HQ Occupancy	Revoked	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:50.783
HQ OIG	Revoked	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:35.567
HQ User Admin	Revoked	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:35.567
HQ OIG	Approved	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:15.63
HQ System Admin	Revoked	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:15.58
HQ Security Admin	Revoked	NA	HEIV01 EIVTest SSOH01	2005-06-22 10:29:15.567

Appendix A – Abbreviations and Acronyms

TERMS, ABBREVIATIONS, AND ACRONYMS

The following terms, abbreviations, and acronyms may or may not appear in this document. They are provided for reference and clarity.

Acronym	Definition
C&A	Certification and Accreditation
CAN	Claim Account Number
CCB	Change Control Board
CCMB	Configuration Change Management Board
CM	Configuration Management
CMRB	Configuration Management Review Board
COTR	Contracting Officer's Technical Representative
DCG	Development Coordination Group
DRP	Disaster Recovery Plan
DTS	Data Transmission Services
EDI	Electronic Data Interchange
EIV	Enterprise Income Verification
FEIN	Federal Employer Identification Number
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FO	Field Office
FOIA	Freedom of Information Act
Form HUD-50058	Form used to submit resident characteristics and tenant income data to HUD
FOUO	For Official Use Only
FTP	File Transfer Protocol
GTM	Government Technical Monitor
GTR	Government Technical Representative
HHS	U.S. Department of Health and Human Services
HOH	Head of Household
HOUSING	Office of Housing
Hub	Not an acronym. FO are classified into two categories -- Hub and Program Center. A Hub can be a stand-alone FO or have another office, a Program Center, report to it.
HUD	US Department of Housing and Urban Development
ICN	Income Control Number
MOA/U	Memorandum of Agreement / Understanding
MTW	Moving To Work
NDNH	National Directory of New Hires
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPC	Office of Procurement & Contracts
PD&R	HUD's Office of Policy, Development and Research
PHA	Public Housing Authorities
PI	Period of Income
PIA	Privacy Act Assessment
PIC	Public & Indian Housing Information Center
PIH	HUD's Office of Public & Indian Housing
POA&M	Plan of Action and Milestones
PVCS	Project Version Control System
PWS	Performance Work Statement

User Role History Report

Acronym	Definition
QA	Quality Assurance
QU	Quarterly Update
QW	Quarterly Wage
RHIIP	Rental Housing Integrity Improvement Project
RIM	Rental Integrity Monitoring
SEIN	State Employment Identification Number
SPH	HUD's Security Program Handbook
SPP	Security Program Policy
SS	Social Security
SSA	Social Security Administration
SSAA	System Security Authorization Agreement
SSI	Supplemental Security Income
SSO	Single Sign On (used in WASS)
SSP	System Security Plan
SWICA	State Wage Income Collection Agency
TARC	Troubled Agency Recovery Center
TARCS	Tenant Rental Assistance Certification System
TASS	Tenant Assessment Subsystem
TRACS	Tenant Rental Assistance Certification System
TTP	Total Tenant Payment
V V&T	Verification, Validation, & Test
W-4	New Hires data
WASS	Web Access Security Subsystem